AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Original) A computer program product for controlling a computer, said computer program product comprising:

malware infection detecting logic operable to detect a malware infection of at least one computer; and

device disabling logic operable upon detection of said malware infection to disable operation of one or more data I/O devices of said at least one computer.

2. (Original) A computer program product as claimed in claim 1, wherein said malware infection detection logic detects a malware infection by one or more of:

positively identifying an item of malware upon said at least one computer; and

identifying behaviour of said at least one computer indicative of malware infection.

3. (Original) A computer program product as claimed in claim 1, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

4. (Original) A computer program product as claimed in claim 1, wherein said device disabling logic is operable upon detection of malware infection to disable at least one data I/O device of at least one further computer.

5. (Original) A computer program product as claimed in claim 1, wherein said device disabling logic is operable to require user confirmation prior to disabling said one or more data I/O devices.

6. (Original) A computer program product as claimed in claim 1, wherein said device disabling logic is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

7. (Currently Amended) A computer program product for controlling a computer, said computer program product comprising:

device disabling logic operable upon receipt by a first computer of a command generated by a second computer indicative of malware infection precautions being taken external to said first computer to disable operation of one or more data I/O devices of said first computer.

8. (Original) A computer program product as claimed in claim 7, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

9. (Currently Amended) A computer program product as claimed in claim 7, wherein said device disabling logic is operable to disable said one or more data I/O devices using an API call to an operating system of said ~~at least one~~ first computer.

10. (Currently Amended) A computer program product for controlling a computer, said computer program product comprising:

user input logic operable to receive at a first computer a user input indicative of activating precautions against a malware infection; and

device disabling logic operable upon receipt of said user input to disable operation of one or more data I/O devices of ~~said at least one~~ a second computer remote from said first computer.

11. (Original) A computer program product as claimed in claim 10, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

12. (Original) A computer program product as claimed in claim 10, wherein said device disabling logic is operable upon detection of malware infection to disable at least one data I/O device of ~~at least one further~~ said second computer.

13. (Original) A computer program product as claimed in claim 10, wherein said device disabling logic is operable to disable said one or more data I/O devices using an API call to an operating system of said ~~at least one~~ second computer.

14. (Original) A method of protecting against malware infection, said method comprising the steps of:

detecting a malware infection of at least one computer; and

upon detection of said malware infection disabling operation of one or more data I/O devices of said at least one computer.

15. (Original) A method as claimed in claim 14, wherein detection of a malware infection is by one or more of:

positively identifying an item of malware upon said at least one computer; and

identifying behaviour of said at least one computer indicative of malware infection.

16. (Original) A method as claimed in claim 14, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

17. (Original) A method as claimed in claim 14, wherein upon detection of malware infection at least one data I/O device of at least one further computer is disabled.

18. (Original) A method as claimed in claim 14, wherein user confirmation is required prior to disabling said one or more data I/O devices.

19. (Original) A method as claimed in claim 14, wherein disabling said one or more data I/O devices uses an API call to an operating system of said at least one computer.

20. (Currently Amended) A method of protecting against malware infection, said method comprising the steps of:

upon receipt by a first computer of a command generated by a second computer indicative of malware infection precautions being taken external to the first computer disabling operation of one or more data I/O devices of said first computer.

21. (Original) A method as claimed in claim 20, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

22. (Currently Amended) A method as claimed in claim 20, wherein disabling said one or more data I/O devices uses an API call to an operating system of said ~~at least one~~ first computer.

23. (Currently Amended) A method of protecting against malware infection, said method comprising the steps of:

receiving at a first computer a user input indicative of activating precautions against a malware infection; and

upon receipt of said user input disabling operation of one or more data I/O devices of ~~said at least one~~ a second computer remote from said first computer.

24. (Original) A method as claimed in claim 23, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

25. (Currently Amended) A method as claimed in claim 23, wherein upon detection of malware infection disabling at least one data I/O device of ~~at least one further~~ said second computer.

26. (Original) A method as claimed in claim 23, wherein disabling said one or more data I/O devices uses an API call to an operating system of said ~~at least one~~ second computer.

27. (Original) Apparatus for protecting against malware infection, said apparatus comprising:

a malware infection detector operable to detect a malware infection of at least one computer; and

a device disabling unit operable upon detection of said malware infection to disable operation of one or more data I/O devices of said at least one computer.

28. (Original) Apparatus as claimed in claim 27, wherein said malware infection detector detects a malware infection by one or more of:

positively identifying an item of malware upon said at least one computer; and

identifying behaviour of said at least one computer indicative of malware infection.

29. (Original) Apparatus as claimed in claim 27, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

30. (Original) Apparatus as claimed in claim 27, wherein said device disabling unit is operable upon detection of malware infection to disable at least one data I/O device of at least one further computer.

31. (Original) Apparatus as claimed in claim 27, wherein said device disabling unit is operable to require user confirmation prior to disabling said one or more data I/O devices.

32. (Original) Apparatus as claimed in claim 27, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

33. (Currently Amended) Apparatus for protecting against malware infection, said apparatus comprising:

a device disabling unit operable upon receipt by a first computer of a command generated by a second computer indicative of malware infection precautions being taken external to the first computer to disable operation of one or more data I/O devices of said first computer.

34. (Original) Apparatus as claimed in claim 33, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

35. (Currently Amended) Apparatus as claimed in claim 33, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said ~~at least one~~ first computer.

36. (Currently Amended) Apparatus for protecting against malware infection, said apparatus comprising:

a user input unit operable to receive at a first computer a user input indicative of activating precautions against a malware infection; and a device disabling unit operable upon receipt of said user input to disable operation of one or more data I/O devices of ~~said at least one~~ a second computer remote from said first computer.

37. (Currently Amended) Apparatus as claimed in claim 36, wherein said one or more data I/O devices include one or more of:

a floppy disk drive;

a compact disk drive;

a removable media drive; and

a network interface card.

38. (Currently Amended) Apparatus as claimed in claim 36, wherein said device disabling unit is operable upon detection of malware infection to disable at least one data I/O device of ~~at least one further~~ a second computer.

39. (Currently Amended) Apparatus as claimed in claim 36, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said ~~at least one~~ second computer.